

What is claimed is:

Sub A. >

1. A method of authenticating information communicated between a first communication device and a second communication device via a communications network, comprising the steps of:
 - a. receiving input data and generating facsimile information in a first format by said first communication device from said input data;
 - b. processing said input data to compute an encrypted checksum;
 - c. convolving said facsimile information with said encrypted checksum data to produce convolved data;
 - d. decrypting, at said second communication device, said encrypted checksum;
 - e. computing a checksum of said input data received at said second communications device; and
 - f. alerting a recipient at said second communication device in the event of a mismatch between said checksum data computed in step (e) and said decrypted checksum data in step (d).
2. The method of claim 1, wherein said first communication device is a digital facsimile apparatus.
3. The method of claim 1, wherein said second communication device is a digital facsimile apparatus.
4. The method of claim 1, wherein said first communication system is a computer system comprising communication means with communication software installed on said computer system.

5. The method of claim 4, wherein a database system is communicatively coupled to said second communication device.

6. The method of claim 1, wherein said second communication system is a computer system comprising communication means with communication software installed in said computer system.

7. The method of claim 26, further comprising the step of:
configuring an e-mail system for receiving and displaying an alert message to said recipient along with said received input data.

8. A method of authenticating the originality of document transmitted by an originating device and received by a destination device through a communication network, comprising the steps of:
scanning a document, intended to be transmitted, and generating information in a first format representative of said document;
calculating an encrypted checksum for said document;
convolving information in said first format with said encrypted checksum, thereby generating data in a second format;
transmitting information in said second format by means of said communication network to said destination device;
computing a checksum of data received by said destination device;
decrypting said encrypted checksum at said destination device; and
comparing said decrypted checksum with computed checksum at said destination device in order to verify the authenticity of data received at said destination device.

9. A system for authenticating information communicated over a network, comprising:

an originating device, said originating device comprising:

means for generating data representative of data received by said originating device;

means for computing a mathematical value representing said input data;

means for encrypting said computed mathematical value, thereby generating an encrypted mathematical value;

means for convolving said representative data and said encrypted mathematical value thereby producing a convolved data;

means for communicating said convolved data to a destination device;

said destination device comprising:

means for computing mathematical value of data received at said destination device;

means for decrypting said mathematical value from said convolved data;

means for comparing said decrypted mathematical value with mathematical value computed by said destination device in order to verify the authenticity of information received by said destination device; and

means for alerting a recipient at said destination device in the event of a mismatch between said decrypted checksum data and the checksum computed by the destination device.